Amendments to the Specification

Page 9, lines 4-7:

Fig. 5 shows the contents of a data set profile 402 or a resource profile 404 in the embodiment shown. As shown in the figure, each profile 402 or 404 contains the name 502 of the data set or resource, the owner 504 of the data set or resource, an access list 506, a universal access authority (UACC) 507~~508~~, and auditing information 508~~510~~.

Page 9, lines 17-20:

The universal access authority (UACC) ~~508~~507 specifies the default access authority, that is, the access authority for a user or group not listed in the access list 506. Like the access authority 606 for a particular user or group, the universal access authority (UACC) ~~508~~507 may be NONE, READ, UPDATE, CONTROL, ALTER, or (for programs) EXECUTE.

Page 10, lines 1-8:

If at step 704 it is determined that the user does not have general superuser authority, then the procedure 700 checks the security manager 316 to determine whether the user has general mount authority, that is, superuser authority for mount operations (step 708). This is done by examining the SUPERUSER.FILESYS.MOUNT resource profile 404 in the UNIXPRIV class of the security database 318 and determining whether the user has at least READ access authority (as indicated by the access list 506 and UACC 507~~508~~). If it is determined that the user does have general mount authority (step 710), then the procedure 700 grants the mount request and allows the mount to occur (step 706).

Page 10, line 21, to page 11, line 3:

If at step 710 it is determined that the user does not have general mount authority, the procedure 700 determines whether the user has mount authority for the specific file system being mounted

(step 712). This is done by examining the data set profile 402 for the data set corresponding the target file system (i.e., the file system being mounted in or unmounted from the other file system) in the security database 318 and determining whether the user either owns the file system (as indicated by the owner field 502) has at least READ access authority to that file system (as indicated by the access list 506 and UACC 507~~508~~); the data set profile 402 examined may be either for the target file system itself or for a data set containing the target file system. If the user does own the target file system or have at least READ access authority to that file system, then the procedure 700 allows the mount to occur (step 706); preferably here, the mount is allowed to occur with the setuid option only if the user owns the target file system. If the user does not own the target file system or have at least READ access authority to that file system, then the procedure 700 denies the mount request and does not allow the mount to occur (step 714).